جرائم الكمبيوتر والانترنت

ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الاجرائية للملاحقة والاثبات

المحامي يونس عرب

ورقة عمل مقدمة الى مؤتمر الامن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية - ابو ظبي 10-12 /2/2002

تمهيد

ان الارقام قد تغني عن الكثير من الأقوال ، واحيانا عن ايجاد مدخل مناسب للحديث عندما تتزاحم العقل افكار عديدة ، ففي احدث تقارير مركز شكاوى احتيال الإنترنت (IFFC) الأمريكي ، اظهر التحليل الشامل للشكاوى التي قدمت للمركز ، ان عدد الشكاوى التي تلقاها المركز منذ بدأ اعماله في ايار 2000 وحتى شهر تشرين ثاني من نفس العام (اي خلال ستة اشهر فقط) قد بلغت 6087 شكوى ، من ضمنها 5273 حالة تتعلق باختراق الكمبيوتر عبر الإنترنت و814 تتعلق بوسائل الدخول والاقتحام الاخرى كالدخول عبر الهاتف او الدخول المباشر الى النظام بشكل مادي ، مع الاشارة الى ان هذه الحالات هي فقط التي تم الابلاغ عنها ولا تمثل الارقام الحقيقية لعدد حالات الاحتيال الفعلي ، وهي تتعلق فقط بجريمة الاحتيال عبر الإنترنت التي هي واحدة من العديد من انماط جرائم الكمبيوتر والإنترنت . وقد بلغت الخسائر المتصلة بهذه الشكاوى ما يقارب 4.6 مليون دولار وهي تقارب 33% من حجم الخسائر الناشئة عن كافة جرائم الاحتيال التقليدية المرتكبة في نفس الفترة . وان 22% من هذه الخسائر نجمت عن شراء منتجات عبر الإنترنت دون ان يتم تسليم البضاعة فعليا للمشترين ، وان 5% منها نشأت عن احتيال بطاقات الائتمان .

ان ظاهرة جرائم الكمبيوتر والانترنت ، او جرائم التقنية العالية ، او الجريمة الإلكترونية ، او (السيبر كرايم- Cyber Crime) ، او جرائم اصحاب الياقات البيضاء White Collar ، ظاهرة اجرامية مستجدة نسبيا تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عنها ، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، (بيانات ومعلومات وبرامج بكافة أنواعها). فهي جريمة تقنية تنشأ في الخفاء يقارفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية ، توجه للنيل من الحق في المعلومات ، وتطال اعتداءاتها معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت . هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة ، وهذا وحده - عبر دلالته العامة - يظهر مدى خطورة جرائم الكمبيوتر ، فهي تطال الحق في المعلومات ، وتمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية وتشيع فقدان الثقة بالتقنية وتهدد ابداع العقل البشري. لذا فان ادراك ماهية جرائم الكمبيوتر والانترنت ، والطبيعة الموضوعية لهذه الجرائم ، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجم عنها وسمات مرتكبيها ودوافعهم ، يتخذ اهمية استثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية .

وإذا كانت مجتمعاتنا العربية لم تتأثر بعد بشكل ملموس بمخاطر هذا النمط المستجد من الإجرام، فان خطر جرائم الكمبيوتر والانترنت المحتمل في البيئة العربية يمكن ان يكون كبيرا باعتبار ان الجاهزية التقنية والتشريعية والادائية (استراتيجيات حماية المعلومات) لمواجهتها ليست بالمستوى المطلوب ان لم تكن غائبة تماما ، وبالمقابل فقد امست جرائم الكمبيوتر والانترنت من أخطر الجرائم التي تقترف في الدول المتقدمة ، تحديدا الأمريكية والأوروبية ، ولهذا تزايدت خطط مكافحة هذه الجرائم وانصبت الجهود على دراستها المتعمقة وخلق آليات قانونية للحماية من إخطارها ، وبرز في هذا المجال المنظمات الدولية والاقليمية خاصة المنظمات والهيئات الإقليمية الأوروبية. وادراكا لقصور القوانين الجنائية بما تتضمنه من نصوص التجريم التقليدية كان لا بد للعديد من الدول من وضع قوانين وتشريعات خاصة ، أو العمل على جبهة قوانينها الداخلية لجهة تعديلها من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم واظهر تحليل الجهود الدولية واتجاهات القانون المقارن بشأن جرائم الكمبيوتر والانترنت ، ان مواجهة هذه الجرائم تم في ثلاثة قطاعات مستقلة ، (حماية استخدام

الكمبيوتر او ما يعرف احيانا بجرائم الكمبيوتر ذات المحتوى الاقتصادي ، وحماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية ، وحماية حق المؤلف على البرامج وقواعد البيانات (الملكية الفكرية للمصنفات الرقمية) وهذا بدوره أضعف امكان صياغة نظرية عامة للحماية الجنائية لتقنية المعلومات. وشتت الجهود بشأن ادراك كنه هذه الظاهرة وصك أدوات ناجحة لمكافحتها ، وهو ما ادى الى توجه الجهود نحو صياغة نظرية عامة لجرائم الكمبيوتر والجرائم التي تستهدف المعلومات ، وهذا ما سعينا شخصيا الى تحقيقه في موسوعة القانون وتقنية المعلومات التي وفقنا الله لوضعها في مؤلفات خمسة تتعدد في بعض الاحيان اجزاء المؤلف الواحد من بينها ، وهو ما كان وراء فكرة انشائنا مركزا متخصصا لبحوث ودراسات القانون تقنية المعلومات (المركز العربي للقانون وتقنية المعلومات) .

ان أكثر مسائل ظاهرة جرائم الكمبيوتر والانترنت اثارة للجدل ، الى جانب تعريفها وتحديد موضوعها او مناط الحماية ومحله ، مسألة تحديد قائمة جرائم الكمبيوتر وتحديد أنماط السلوك الاجرامي والأفعال المكونة له ، وتبين القوام القانوني لهذه الجرائم ، هذه المسألة أفرزت خلافا وتباينا موضوعيا لدى الفقه الجنائي في مختلف النظم القانونية ، اللاتينية والجرمانيه والانجلوسكونية ، حول مدى انطباق نصوص القوانين الجنائية التقليدية على هذه الجرائم - على الاقل في السنوات الاولى لبروز الظاهرة وقبل ان تتجه الاراء للحسم لجهة عدم قابلية النصوص القائمة او عجزها وعدم كفايتها للانطباق على هذه الانماط الجديدة من الجرائم . واذا كنا ممن تبنى في عام 1994 – ضمن رسالتنا لنيل درجة الماجستير في جرائم الحاسوب - الرأي القائل بعدم امكان تطبيق النصوص القائمة ، فان تطور ظاهرة جرائم الكمبيوتر وتنامي الدراسات البحثية في هذا الحقل اظهر سلامة وصحة هذا الموقف الذي اتجه ويتجه له في وقتنا الحاضر غالبية فقهاء ودارسي وباحثي القانون الجنائي وتحديدا فقه قانون امن المعلومات .

ان هذه الورقة مجرد اطار عام وموجز للمسائل ذات الصلة بتحديد انماط جرائم الكمبيوتر والانترنت وفعالية اجراءات مكافحتها ، ونقول اطار عام لان المقام لا يتسع لعرض مختلف هذه المسائل او تناولها تفصيلا ، آملين ان يكون هذا المؤتمر واحدا من تلك المؤتمرات التي ادت الى صياغة تحولات حقيقة في فهم الظاهرة وتحديد متطلبات معالجتها وآملين ان تحقق الورقة غايتها محيلين القاريء الكريم الى مؤلفنا المتخصص في هذا الحقل

1- ما المقصود بجرائم الكمبيوتر والإنترنت؟

تعرف الجريمة عموما، في نطاق القانون الجنائي - الذي يطلق عليه أيضا تسميات قانون الجزاء وقانون العقوبات وينهض بكل تسمية حجج وأسانيد ليس المقام عرضها بأنها "فعل غير مشروع صادر عن ارادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا". وعلى الرغم من التباين الكبير في تعريفات الجريمة بين الفقهاء القانونين وبينهم وبين علماء الاجتماع الا أننا تخيرنا هذا التعريف استنادا الى أن التعريف الكامل -كما يرى الفقه - هو ما حدد عناصر الجريمة الى جانب بيانه لأثرها ونود ابتداء التأكيد على أهمية هذه القاعدة في تعريف الجريمة ، فبيان عناصر الجريمة (السلوك، والسلوك غير المشروع وفق القانون، الارادة الجنائية ، وأثرها - العقوبة أو التدبير الذي يفرضه القانون) من شأنه في الحقيقة أن يعطي تعريفا دقيقا لوصف الجريمة عموما، ويمايز بينها وبين الأفعال المستهجنة في نطاق الأخلاق ، أو الجرائم المدنية أو الجرائم التأديبية.

أما جريمة الكمبيوتر ، فقد صك الفقهاء والدارسون لها عددا ليس بالقليل من التعريفات، تتمايز وتتباين تبعا لموضع العلم المنتمية اليه وتبعا لمعيار التعريف ذاته ، فاختلفت بين أولئك الباحثين في الظاهرة الاجرامية الناشئة عن استخدام الكمبيوتر من الوجهة التقنية وأولئك الباحثين في ذات الظاهرة من الوجهة القانونية ، وفي الطائفة الأخيرة -محل اهتمامنا الرئيسي- تباينت التعريفات تبعا لموضوع الدراسة (القانونية) ذاته ، وتعددت حسب ما اذا كانت الدراسة متعلقة بالقانون الجنائي أم متصلة بالحياة الخاصة أم متعلقة بحقوق الملكية الفكرية (حق التأليف على البرامج).

وقد خلت الدراسات والمؤلفات التي في هذا الحقل (قديمها وحديثها) من تناول اتجاهات الفقه في تعريف جريمة الكمبيوتر عدا مؤلفين ، في البيئة العربية ، اما في البيئة المقارنة نجد مؤلفات الفقيه Ulrich Sieber اهتمت بتقصي مختلف التعريفات التي وضعت لجرائم الكمبيوتر . وقد اجتهدنا في عام 1994 في جمع غالبية التعريفات التي وضعت في هذا الحقل واوجدنا تصنيفا خاصا لها لمحاولة تحري اكثرها دقة في التعبير عن هذه الظاهرة، وبغض النظر عن المصطلح المستخدم للدلالة على جرائم الكمبيوتر والإنترنت فقد قمنا في الموضع المشار اليه بتقسيم هذه التعريفات – حتى ذلك التاريخ - الى طائفتين رئيستين : - أولهما ، طائفة التعريفات التي تقوم على معيار واحد ، وهذه تشمل تعريفات قائمة على معيار قانوني ، كتعريفها بدلالة موضوع الجريمة او السلوك محل التجريم او الوسيلة المستخدمة ، وتشمل أيضا تعريفات قائمة على معيار شخصي ، وتحديدا متطلب توفر المعرفة والدراية التقنية لدى شخص مرتكبها. وثانيهما ، طائفة التعريفات القائمة على تعدد المعايير ، وتشمل التعريفات التي تبرز موضوع الجريمة وانماطها وبعض العناصر المتصلة باليات ارتكابها او بيئة ارتكابها او سمات مرتكبها .

ولا نقف في هذا المقام على العرض التفصيلي للمسائل المتقدم الاشارة اليها ، ونكتفي بابراز بعض التعريفات ثم عرض النتائج بشانها على ان يعرف القاريء الكريم انه مجرد استعراض موجز ولمزيد من الاطلاع يمكن الرجوع للمراجع المتخصصة المشار اليها في هذه الورقة وما عرضناه تفصيلا في مؤلفنا جرائم الكمبيوتر والانترنت السابق الاشارة اليه .

من التعريفات التي تستند الى موضوع الجريمة او احيانا الى انماط السلوك محل التجريم ، تعريفها بانها " نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه "وتعريفها بانها " كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات " او هي " أي نمط من انماط الجرائم المعروف في قانون العقوبات طالما

كان مرتبطا بتقنية المعلومات "او هي " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة واساءة استخدام المخرجات اضافة الى أفعال أخرى تشكل جرائم اكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر "

اما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة ، فان اصحابها ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة ، من هذه التعريفات ، يعرفها الأستاذ جون فورسترووكذلك الأستاذ Eslie D. Ball أنها " فعل اجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" ويعرفها تاديمان Tiedemaun بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكذلك يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا" جانب من الفقه والمؤسسات ذات العلاقة بهذا الموضوع ، وضعت عددا من التعريفات التي تقوم على اساس سمات شخصية لدى مرتكب الفعل ، وهي تحديدا سمة الدراية والمعرفة التقنية . من هذه التعريفات ، تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للابحاث وتبنتها الوزارة في دليلها لعام 1979 ، حيث عرفت بانها " اية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها " . ومن هذه التعريفات أيضا تعريف David Thompson بانها " اية جريمة يكون متطلبا لاقترافها ان تتوافر لدى فاعلها معرفة بتقنية الحاسب " . وتعريف Stein Schjqlberg بانها " أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر اساسية لارتكابه والتحقيق فيه وملاحقته قضائيا "

كما يعرفها الأستاذ Sheldon. J. Hecht بأنها: "واقعة تتضمن تقنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب" وقريب منه تعريف الفقيهDonn B. Parker في مؤلفه Fighting Computer Crime والذي يرى بأنها "أي فعل متعمد مرتبط بأي وجه، بالحاسبات، يتسبب في تكبد أو امكانية تكبد مجني عليه لخسارة أو حصول أو امكانية حصول مرتكبه على مكسب" ويستخدم للدلالة على الجريمة تعبير "إساءة استخدام الحاسوب".

وقد عرف جريمة الكمبيوتر خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD ، بانها " كل فعل او امتناع من شانه الاعتداء على الأمواج المادية او المعنوية يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية " والتعريف البلجيكي السالف، متبنى من قبل العديد من الفقهاء والدارسين بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الاحاطة الشاملة قدر الامكان بظاهرة جرائم التقنية ، ولأن التعريف المذكور يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، ولأنه أخيرا يتيح امكانية التعامل مع التطورات المستقبلية التقنية.

ان الجرائم التي تطال ماديات الكمبيوتر ووسائل الاتصال ، شأنها شأن الجرائم المستقرة على مدى قرنين من التشريع الجنائي، محلها أموال مادية صيغت على أساس صفتها نظريات وقواعد ونصوص القانون الجنائي على عكس (معنويات) الكمبيوتر ووسائل تقنية المعلومات ، التي أفرزت أنشطة الاعتداء عليها تساؤلا عريضا - تكاد تنحسم الاجابة عليه بالنفي- حول مدى انطباق نصوص القانون الجنائي التقليدية عليه.

ويعرف خبراء منظمة التعاون الاقتصادي والتنمية، جريمة الكمبيوتر بأنها :

"كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/ أو نقلها" وقد وضع هذا التعريف من قبل مجموعة الخبراء المشار اليهم للنقاش في اجتماع باريس الذي عقد عام 1983 ضمن حلقة (الاجرام المرتبط بتقنية المعلومات)، ويتبنى هذا التعريف الفقيه الالماني Ulrich Sieher ، ويعتمد هذا التعريف على معيارين : أولهما، (وصف السلوك). وثانيهما، اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

ومن ضمن التعريفات التي تعتمد أكثر من معيار، يعرف جانب من الفقه جريمة الكمبيوتر وفق معايير قانونية صرفه ، أولها تحديد محل الجريمة، وثانيها وسيلة ارتكابها وهو في كلا المعيارين (الكمبيوتر) لما يلعبه من دور الضحية ودور الوسيلة حسب الفعل المرتكب كما يرى هذا الجانب من الفقه. من هؤلاء الأستاذ Thomas. J. Smedinghoff في مؤلفه (المرشد القانوني لتطوير وحماية وتسويق البرمجيات). حيث يعرفها بأنها "أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسوب". وكما أسلفنا فتعبير (النشاط الموجه ضد) ينسحب على الكيانات المادية اضافة للمنطقية (المعطيات والبرامج). وكذلك تعريف الأستاذين Robert J. Lindquist و Jack Bologna " جريمة يستخدم الحاسوب كوسيلة mens أو أداة Instrument لارتكابها أو يمثل اغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها" .

ومن الفقه الفرنسي، يعرف الفقيه Masse جريمة الكمبيوتر (يستخدم اصطلاح الغش المعلوماتي) بأنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح" وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال .

ويعرفها الفقهيين الفرنسيين Le stanc, Vivant بأنها : "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب".

تقدير

لقد غرقت بعض التعريفات في التعامل مع جرائم الكمبيوتر كجرائم خاصة دون الاجابة مسبقا على موقع هذه الجرائم في نطاق القانون الجنائي ، بمعنى اذا كنا أمام ظاهرة اجرامية مستجدة تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها وأنماط السلوك الاجرامي المجسدة للركن المادي لكل جريمة من هذه الجرائم ، أفلا يستدعي ذلك صياغة نظرية عامة لهذه الجرائم؟؟

هذه النظرية (العامة) ، أهي نظرية جنائية في نطاق القسم الخاص من قانون العقوبات ، لا تخلق اشكالات واسعة على الاقل - في تطبيق قواعد ونظريات القسم العام من قانون العقوبات ؟؟ أم ان هذه النظرية يجب أن تؤسس لقواعد وأحكام حديثة تطال قسمي القانون الخاص والعام؟!.

يقول د. محمود نجيب حسني :

"ثمة نظريات للقسم الخاص لا صلة بينها وبين تطبيق القسم العام، ويكفي أن نشير الى نظريات العلانية في جرائم الاعتبار (الفعل الفاضح والسب)، والضرر في جرائم التزوير، والحيازة في السرقة والتدليس في النصب... لقد انتجت دراسة القسم الخاص نظريات لا تقل من حيث الخصوبة عن نظريات القسم العام...وعليه، يمكن القول بوجود نظريات عامة للقسم الخاص"

ان طبيعة وأبعاد ظاهرة جرائم الكمبيوتر ، سيما في ظل تطور انماطها يوما بعد يوم مع تطور استخدام الشبكات وما اتاحته الإنترنت من فرص جديدة لارتكابها وخلقت انماطا مستجدة لها يشير الى تميزها في احكام لا توفرها النظريات القائمة ، تحديدا مسائل محل الاعتداء والسلوكيات المادية المتصلة بارتكاب الجرم ، وهذا ما أدى الى حسم الجدل الواسع حول مدى انطباق النصوص القائمة على هذه الجرائم لجهة وضع تشريعات ونصوص جديدة تكون قادرة على الاحاطة بمفردات ومتطلبات وخصوصية جرائم الكمبيوتر والإنترنت ، وهو بالتالي ما يحسم الجدل حول الحاجة الى نظرية عامة لجرائم الكمبيوتر توقف التوصيف الجزئي والمعالجات المبتسرة .

ولا بد من التمييز في التعريف بين ظاهرة اجرام الحوسبة، أو كما يسميها قطاع واسع من الفقه المصري ظاهرة الجناح أو الانحراف المعلوماتي وبين جرائم الكمبيوتر والإنترنت . فتعريف الظاهرة مؤسس على مرتكزات عريضة وواسعة، هي في الغالب تعطي دلالة محل الظاهرة لكنها لا تنهض بايضاح هذا المحل على نحو عميق وشامل ووفق مرتكزات التعريف المطلوب في نطاق القانون الجنائي . أما تعريف الجريمة (عموما)، فكما ذكرنا إعلانية ، تتحقق فعاليته اذا ما أورد عناصرها وأثرها ، في حين أن التعريف لجريمة معينة يتطلب اظهار ركنها المادي المتمثل بالسلوك الاجرامي بشكل أساسي اضافة الى ما يتطلبه أحيانا من ايراد صورة الركن المعنوي أو العنصر المفترض أو غير ذلك.

وبالتالي فان الاعتداء على كيانات الاجهزة التقنية المادية (يتعدد وصفها ومهامها من الوجهة التقنية) يخرج من نطاق جرائم الكمبيوتر لترتد الى موقعها الطبيعي ، وهو الجرائم التقليدية ، باعتبار هذه الماديات مجسدة لمال منقول مادي تنهض به قواعد ومبادئ ونصوص القانون الجنائي واذا كان من وجوب الحديث عن الاعتداءات على الكيانات المادية في نطاق ظاهرة جرائم الكمبيوتر والإنترنت ، فانه متعلق فقط بقيمتها الاستراتيجية كمخازن للمعلومات وأدوات لمعالجتها وتبادلها ، مما يستدعي نقاش تطوير آليات حمايتها ، خاصة من أنشطة الإرهاب والتخريب المعادية للتقنية (كموقف سياسي او ايديولوجي) ولكن في نطاق النصوص التقليدية لا في نطاق ظاهرة جرائم الكمبيوتر المستجدة ، مع التنبه الى ان أفعال الاتلاف والتدمير المرتكبة في نطاق جرائم الكمبيوتر والإنترنت ، هي الموجهة للنظم والمعطيات وليس لماديات الاجهزة .

اما عن دور الكمبيوتر في الجريمة ، فانه متعدد في الحقيقة ، فهو اما ان يكون الهدف المباشر للاعتداء ، او هو وسيلة الاعتداء لتحقيق نتيجة جرمية لا تتصل مباشرة بالمعطيات وانما بما تمثله او تجسده ، او هو بيئة ومخزن للجريمة ، ويجب أن لا يوقعنا أي من هذه الادوار في أي خلط بشان محل الجريمة أو وسيلة ارتكابها، فان محل جريمة دائما هو المعطيات (أما بذاتها أو بما تمثله) ووسيلة ارتكاب جريمة الكمبيوتر والإنترنت الكمبيوتر او أي من الاجهزة التكاملية التقنية (أي التي تدمج بين تقنيات الاتصال والحوسبة) وعلى أن يراعى ان دلالة نظام الكمبيوتر تشمل نظم تقنية المعلومات المجسدة في الكمبيوتر المحقق لتوأمة الحوسبة والاتصال في عصر التقنية الشاملة المتقاربة.

واذا كانت تعريفات الجريمة عموما تقوم على أساسين : عناصر الجريمة و السلوك ووصفه، والنص القانوني على تجريم السلوك وايقاع العقوبة، فان الجديد في مجال جرائم الكمبيوتر هو اضافة عنصر ثالث يبرز محل الاعتداء في هذه الظاهرة الاجرامية المستحدثة ، متمثلا بمعطيات الحاسوب. فقانون العقوبات ينطوي على نصوص تحرم الاعتداء على الأشخاص ، الأموال ، الثقة العامة ... الخ ، لكن المستجد ، هو الكيانات المعنوية ذات القيمة المالية أو القيمة المعنوية البحتة، أو كلاهما، ولولا هذه الطبيعة المستجدة في الأساس لما كنا أمام ظاهرة مستجدة برمتها، ولكان المستجد هو دخول الكمبيوتر عالم الاجرام ، تماما كما هو الشأن في الجرائم المنظمة، فهي في الحقيقة جرائم تقليدية المستجد فيها عنصر التنظيم الذي ينتج مخاطر هائلة واتساع نطاق المساهمة الجنائية وانصهار الارادات الجرمية في ارادة واحدة هي ارادة المنظمة الاجرامية المعنية .

وعلينا التاكيد هنا على ان جرائم الكمبيوتر ليست مجرد جرائم تقليدية بثوب جديد او بوسيلة جدية فهذا قد ينطبق على بعض صور الجرائم التي يكون الكمبيوتر فيها وسيلة لارتكاب الجريمة ، وليس صحيحا ما قاله الكثير من الاعلاميين الغربيين في المراحل الأولى لظاهرة الكمبيوتر انها ليست اكثر من (نبيذ قديم في زجاجة جديدة) . انها بحق ، جرائم جديدة في محتواها ونطاقها ومخاطرها ، ووسائلها ، ومشكلاتها ، وفي الغالب في طبائع وسمات مرتكبيها .

على ضوء ما تقدم من استخلاصات واستنتاجات فاننا في معرض تحديد ماهية هذه الجرائم والوقوف على تعريفها ، نخلص للنتائج التالية :-

ان الاعتداء على الكيانات المادية للكمبيوتر وأجهزة الاتصال يخرج عن نطاق جرائم الكمبيوتر لان هذه الكيانات محل صالح لتطبيق نصوص التجريم التقليدية المنظمة لجرائم السرقة والاحتيال واساءة الامانة والتدمير والاتلاف وغير ذلك ، باعتبار ان هذه السلوكيات تقع على مال مادي منقول ، والأجهزة تنتسب الى هذا النطاق من الوصف كمحل للجريمة .

ان مفهوم جريمة الكمبيوتر مر بتطور تاريخي تبعا لتطور التقنية واستخداماتها ، ففي المرحلة الأولى من شيوع استخدام الكمبيوتر في الستينات ومن ثم السبعينات ، ظهرت اول معالجات لما يسمى جرائم الكمبيوتر - وكان ذلك في الستينات - واقتصرت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر ، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة جرمية مستجدة ، بل ثار الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير اخلاقية في بيئة او مهنة الحوسبة ، وبقي التعامل معها اقرب الى النطاق الاخلاقي منه الى النطاق القانوني ، ومع تزايد استخدام الحواسيب الشخصية في منتصف السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية ، وبدأ الحديث عنها بوصفها ظاهرة جرمية لا مجرد سلوكيات مرفوضة . وفي الثمانينات طفا على السطح مفهوم جديد لجرائم الكمبيوتر ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد وانشطة نشر وزراعة الفايروسات الإلكترونية ، التي تقوم بعمليات تدميرية للملفات او البرامج ، وشاع اصطلاح (الهاكرز) المعبر عن مقتحمي النظم ، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل في غالب الاحيان محصورا بالحديث عن رغبة المخترقين في تجاوز إجراءات أمن المعلومات وفي اظهار تفوقهم التقني ، وانحصر الحديث عن مرتكبي الأفعال هذه بالحديث عن صغار السن من المتفوقين الراغبين بالتحدي والمغامرة والى مدى نشأت معه قواعد سلوكية لهيئات ومنظمات الهاكرز طالبوا معها بوقف تشويه حقيقتهم واصرارهم على انهم يؤدون خدمة في التوعية لأهمية معايير أمن النظم والمعلومات لكن الحقيقة ان مغامري الامس اصبحوا عتاة اجرام فيما بعد ، الى حد إعادة النظر في تحديد سمات مرتكبي الجرائم وطوائفهم ، وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض جرمية خطرة ، القادر على ارتكاب أفعال تستهدف الاستيلاء على المال او تستهدف التجسس او الاستيلاء على البيانات السرية الاقتصادية والاجتماعية والسياسية والعسكرية . وشهدت التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها ، وكان ذلك بفعل ما احدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات ، فظهرت انماط جديدة كانشطة انكار الخدمة التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد ، واكثر ما مورست ضد مواقع الإنترنت التسويقية الناشطة والهامة التي يعني انقطاعها عن الخدمة لساعات خسائر مالية بالملايين . ونشطت جرائم نشر الفايروسات عبر مواقع الإنترنت لما تسهله من انتقالها الى ملايين المستخدمين في ذات الوقت ، وظهرت انشطة الرسائل والمواد الكتابية المنشورة على الإنترنت او المرسلة عبر البريد الإلكتروني المنطوية على اثارة الاحقاد او المساس بكرامة واعتبار الأشخاص او المستهدفة الترويج لمواد او أفعال غير قانونية وغير مشروعة (جرائم المحتوى الضار).

ان محل جريمة الكمبيوتر هو دائما المعطيات اما بذاتها او بما تمثله هذه المعطيات التي قد تكون مخزنة داخل النظام او على أحد وسائط التخزين او تكون في طور النقل والتبادل ضمن وسائل الاتصال المندمجة مع نظام الحوسبة .

ان كل جرم يمس مصلحة يقدر الشارع اهمية التدخل لحمايتها ، والمصلحة محل الحماية في ميدان جرائم الكمبيوتر هي الحق في المعلومات (كعنصر معنوي ذي قيمة اقتصادية عاليـة) ويشمل ذلك الحق في الوصول الى المعلومات وانسيابها وتدفقها وتبادلها وتنظيم استخدامها كل ذلك على نحو مشروع ودون مساس بحقوق الآخرين في المعلومات .

ان تعريف الجريمة عموما يتأسس على بيان عناصرها المناط بالقانون تحديدها ، اذ من دون نص القانون على النموذج القانوني للجريمة لا يتحقق امكان المساءلة عنها (سندا الى قاعدة الشرعية الجنائية التي توجب عدم جواز العقاب عند انتفاء النص ، وسندا الى ان القياس محظور في ميدان النصوص التجريمية الموضوعية) ، وهو ما يستوجب التمييز بين الظاهرة الجرمية والجريمة . ولذلك فان ظاهرة جرائم الكمبيوتر تعرف وفق التحديد المتقدم بانها (الأفعال غير المشروعة المرتبطة بنظم الحواسيب) اما تعريف جريمة الكمبيوتر فانها (سلوك غير مشروع معاقب عليه قانونا صادر عن ارادة جرمية محله معطيات الكمبيوتر) فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل ، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية ، ومعاقب عليه قانونا لان اسباغ الصفة الاجرامية لا يتحقق في ميدان القانون الجنائي الا بارادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفا للاخلاق . ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة ، بيانات ومعلومات معالجة ومخزنة ، البرامج بانواعها ، المعلومات المستخرجة ، والمتبادلة بين النظم) واما الكمبيوتر فهو النظام التقني بمفهومه الشامل المزاوج بين تقنيات الحوسبة والاتصال ، بما في ذلك شبكات المعلومات.

2- دور الكمبيوتر في الجريمة

يلعب الكمبيوتر ثلاثة ادوار في ميدان ارتكاب الجرائم ، ودورا رئيسا في حقل اكتشافها ، ففي حقل ارتكاب الجرائم يكون للكمبيوتر الادوار التالية :-

الاول:- قد يكون الكمبيوتر هدفا للجريمة (Target of an offense) ، وذلك كما في حالة الدخول غير المصرح به الى النظام او زراعة الفايروسات لتدمير المعطيات والملفات المخزنة او تعديلها ، وكما في حالة الاستيلاء على البيانات المخزنة او المنقولة عبر النظم.

ومن اوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية ، عندما تكون السرية (CONFIDENTIALITY) والتكاملية أي السلامة (INTEGRITY) والقدرة أو التوفر (AVAILABILITY) هي التي يتم الاعتداء عليها ، بمعنى ان توجه هجمات الكمبيوتر الى معلومات الكمبيوتر او خدماته بقصد المساس بالسرية او المساس بالسلامة والمحتوى والتكاملية ، او تعطيل القدرة والكفاءة للانظمة للقيام باعمالها ، وهدف هذا النمط الاجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون تخويل ودون ان يدفع الشخص مقابل الاستخدام (سرقة خدمات الكمبيوتر ، او وقت الكمبيوتر) او المساس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر وغالبية هذه الأفعال الجرمية تتضمن ابتداءا الدخول غير المصرح به الى النظام الهدف (UNAUTHORIZED ACCESS) والتي توصف بشكل شائع في هذه الايام بأنشطة الهاكرز كناية عن فعل الاختراق (HACKING

والافعال التي تتضمن سرقة للمعلومات تتخذ اشكال عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء ، فالكمبيوترات مخازن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق وغيرها وهذه تمثل هدفا للعديد من الجهات بما فيها ايضا جهات التحقيق الجنائي والمنظمات الارهابية وجهات المخابرات والاجهزة الامنية وغيرها ، ولا يتوقف نشاط الاختراق على الملفات والانظمة غير الحكومية بل يمتد الى الانظمة الخاصة التي تتضمن بيانات قيمة ، فعلى سبيل المثال قد يتوصل احد المخترقين للدخول الى نظام الحجز في احد الفنادق لسرقة ارقام بطاقات الائتمان . وتتضمن بعض طوائف هذا النمط أي الكمبيوتر كهدف انشطة سرقة والاعتداء على الملكية الفكرية كسرقة الاسرار التجارية واعادة انتاج ونسخ المصنفات المحمية وتحديدا برامج الحاسوب . وفي حالات اخرى فان افعال الاختراق التي تستهدف انظمة المعلومات الخاصة تستهدف منافع تجارية او ارضاء اطماع شخصية كما ان الهدف في هذه الطائفة يتضمن انظمة سجلات طبية وانظمة الهاتف وسجلاته ونماذج تعبئة البيانات للمستهلكين وغيرها .

الثاني :- وقد يكون الكمبيوتر اداة الجريمة لارتكـــاب جرائم تقليدية A tool in the commission of a traditional offense

كما في حالة استغلال الكمبيوتر للاستيلاء على الأموال باجراء تحويلات غير مشروعة او استخدام التقنية في عمليات التزييف والتزوير ، او استخدام التقنية في الاستيلاء على ارقام بطاقات ائتمان واعادة استخدامها والاستيلاء على الاموال بواسطة ذلك ، حتى ان الكمبيوتر كوسيلة قد يستخدم في جرائم القتل ، كما في الدخول الى قواعد البيانات الصحية والعلاجية وتحويرها او تحوير عمل الاجهزة الطبية والمخبرية عبر التلاعب ببرمجياتها ، او كما في اتباع الوسائل الالكترونية للتأثير على عمل برمجيات التحكم في الطائرة او السفينة بشكل يؤدي الى تدميرها وقتل ركابها .

الثالث :- وقد يكون الكمبيوتر بيئة الجريمة ، وذلك كما في تخزين البرامج المقرصنة فيه او في حالة استخدامه لنشر المواد غير القانونية او استخدامه اداة تخزين او اتصال لصفقات ترويج المخدرات وانشطة الشبكات الاباحية ونحوها .

وطبعا يمكن للكمبيوتر ان يلعب الادوار الثلاثة معا ، ومثال ذلك ان يستخدم احد مخترقي الكمبيوتر (هاكرز) جهازه للتوصل دون تصريح الى نظام مزود خدمات انترنت (مثل نظام شركة امريكا اون لاين) ومن ثم يستخدم الدخول غير القانوني لتوزيع برنامج مخزن في نظامه (أي نظام المخترق) فهو قد ارتكب فعلا موجها نحو الكمبيوتر بوصفه هدفا (الدخول غير المصرح به) ثم استخدم الكمبيوتر لنشاط جرمي تقليدي (عرض وتوزيع المصنفات المقرصنة) واستخدم كمبيوتره كبيئة او مخزن للجريمة عندما قام بتوزيع برنامج مخزن في نظامه .

اما من حيث دور الكمبيوتر في اكتشاف الجريمة ، فان الكمبيوتر يستخدم الان على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم ، عوضا عن ان جهات تنفيذ القانون تعتمد على النظم التقنية في ادارة المهام من خلال بناء قواعد البيانات ضمن جهاز ادارة العدالة والتطبيق القانوني ، ومع تزايد نطاق جرائم الكمبيوتر ، واعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة ، فانه اصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها ، من هنا يلعب الكمبيوتر ذاته دورا رئيسا في كشف جرائم الكمبيوتر وتتبع فاعليها بل وابطال اثر الهجمات التدميرية لمخترقي النظم وتحديدا هجمات الفيروسات وإنكار الخدمة وقرصنة البرمجيات .

طوائف جرائم الكمبيوتر والانترنت وفق المدونات الدولية والاقليمية والوطنية المقارنة .

يصنف الفقهاء والدارسون جرائم الحاسوب ضمن فئات متعددة، تختلف حسب الأساس والمعيار الذي يستند اليه التقسيم المعني ، فبعضهم يقسمها الى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته ، وبعضهم يصنفها ضمن فئات بالاستناد الى الأسلوب المتبع في الجريمة، وآخرون يستندون الى الباعث أو الدافع لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، وكذا تعدد الحق المعتدى عليه فتوزع جرائم الحاسوب وفق هذا التقسيم الى جرائم تقع على الأموال بواسطة الحاسوب وتلك التي تقع على الحياة الخاصة.

ومن الملاحظ أن هذه التقسيمات أو بعضها، لم تراع بعض أو كل خصائص هذه الجرائم وموضوعها، والحق المعتدى عليه لدى وضعها لأساس أو معيار التقسيم، وقد تناولنا غالبية ما يتصل بهذا الموضوع فيما تقدم ، وخلصنا الى أن جرائم الحاسوب في نطاق الظاهرة الاجرامية المستحدثة، جرائم تنصب على معطيات الحاسوب (بيانات ومعلومات وبرامج) وتطال الحق في المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب، والى ان الجرائم التي تنصب على الكيانات المادية مما يدخل في نطاق الجرائم التقليدية ولا يندرج ضمن الظاهرة المستجدة لجرائم الحاسوب.

ولا نبالغ ان قلنا ان ثمة نظريات ومعايير لتصنيف طوائف جرائم الكمبيوتر والانترنت بعدد مؤلفي وباحثي هذا الفرع القانوني ، ومصدر هذا التعدد التباين في رؤية دور الكمبيوتر ومحاولات وصف الافعال الجرمية بوسائل ارتكابها ، ومع هذا سنحاول ان نقف على ابرز التصنيفات بهدف الاحاطة بمختلف الانماط التي ستكون محل دراسة في الفصل اللاحق .

تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة .

هذا التصنيف هو الذي ترافق مع موجات التشريع في ميدان قانون تقنية المعلومات ، وهو التصنيف الذي يعكس ايضا التطور التاريخي لظاهرة جرائم الكمبيوتر والانترنت ، ونجده التصنيف السائد في مختلف مؤلفات الفقيه الريش سيبر والمؤلفات المتاثرة به ولهذا نجد أن جرائم الحاسوب بالاستناد الى هذا المعيار يمكن تقسيمها ضمن الطوائف التالية :-

أولا : الجرائم الماسة بقيمة معطيات الحاسوب، وتشمل هذه الطائفة فئتين، أولهما، الجرائم الواقعة على ذات المعطيات، كجرائم الاتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة (الفيروسات) التقنية. وثانيهما، الجرائم الواقعة على ما تمثله المعطيات آليا، من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات ، وجرائم التحوير والتلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها (تزوير المستندات المعالجة آليا واستخدامها).

ثانيا : الجرائم الماسة بالمعطيات الشخصية او البيانات المتصلة بالحياة الخاصة ، وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة،

ثالثا : الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات) التي تشمل نسخ وتقليد البرامج واعادة انتاجها وصنعها دون ترخيص والاعتداء على العلامة التجارية وبراءة الاختراع.

وبامعان النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومتحقق، اذ أن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن الغرض المباشر المحرك للاعتداء انصب على قيمتها أو ما تمثله. والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي) لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج.

هذا من جهة، ومن جهة أخرى، نجد أن الحماية الجنائية للمعلومات في نطاق القانون المقارن وفي اطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت على نحو غالب، التقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج ، وحماية البيانات الشخصية المتصلة بالحياة الخاصة وحماية المعطيات بالنظر لقيمتها أو ما تمثله والذي عرف بحماية (الأموال)، كل في ميدان وموقع مستقل. وهو في الحقيقة تمييز - ليس مطلقا - بين حماية قيمة المعطيات، وأمنها، وحقوق الملكية الفكرية. ولا بد لنا من الاشارة، ان حماية أمن المعطيات (الطائفة الثانية) انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة، أما حماية البيانات والمعلومات السرية والمحمية فقد تم تناوله في نطاق جرائم الطائفة الأولى الماسة بقيمة المعطيات بالنظر الى أن الباعث الرئيسي للاعتداء والغرض من معرفة أو افشاء هذه المعلومات غالبا ما كان الحصول على المال مما يعد من الاعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم.

تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة .

عرضنا فيما تقدم لدور الكمبيوتر في الجريمة ، فقد يكون هدف الاعتداء ، بمعنى ان يستهدف الفعل المعطيات المعالجة او المخزنة او المتبادلة بواسطة الكمبيوتر والشبكات ، وهذا ما يعبر عنه بالمفهوم الضيق (لجرائم الكمبيوتر) وقد يكون الكمبيوتر وسيلة ارتكاب جريمة اخرى في اطار مفهوم (الجرائم المرتبطة بالكمبيوتر) ، وقد يكون الكمبيوتر اخيرا بيئة الجريمة او وسطها او مخزنا للمادة الجرمية ، وفي هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن هذا الدور الاول جرائم التخزين ، ويقصد بها تخزين المواد الجرمية او المستخدمة في ارتكاب الجريمة او الناشئة عنها ، والثاني ، جرائم المحتوى او ما يعبر عنه بالمحتوى غير المشروع او غير القانوني والاصطلاح الاخير استخدم في ضوء تطور اشكال الجريمة مع استخدام الانترنت ، واصبح المحتوى غير القانوني يرمز الى جرائم المقامرة ونشر المواد الاباحية والغسيل الالكتروني للاموال وغيرها باعتبار ان مواقع الانترنت تتصل بشكل رئيس بهذه الانشطة ، والحقيقة ان كلا المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفي نفس الوقت كوسيلة لارتكابها . وهذا التقسيم شائع بجزء منه (وهو تقسيم الجرائم الى جرائم هدف ووسيلة) لدى الفقه المصري والفرنسي وتبعا له تنقسم جرائم الكمبيوتر الى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات واتلافها ، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر . اما تقسيمها كجرائم هدف ووسيلة ومحتوى فانه الاتجاه العالمي الجديد في ضوء تطور التدابير التشريعية في اوروبا تحديدا ، وافضل ما يعكس هذا التقسيم الاتفاقية الاوروبية لجرائم الكمبيوتر والانترنت لعام 2001 – ذلك ان العمل منذ مطلع عام 2000 يتجه الى وضع اطار عام لتصنيف جرائم الكمبيوتر والانترنت وعلى الاقل وضع قائمة الحد الادنى محل التعاون الدولي في حقل مكافحة هذه الجرائم ، وهو جهد تقوده دول اوروبا لكن وبنفس الوقت بتدخل ومساهمة من قبل استراليا وكندا وامريكا ، وضمن هذا المفهوم نجد الاتفاقية المشار اليها تقسم جرائم الكمبيوتر والانترنت الى الطوائف التالية – مع ملاحظة انها تخرج من بينها طائفة جرائم الخصوصية لوجود اتفاقية اوروبية مستقلة تعالج حماية البيانات الاسمية من مخاطر المعالجة الالية للبيانات – اتفاقية 1981 ، على نحو ما عالجنا تفصيلا في مؤلفنا جرائم الكمبيوتر والانترنت .

لقد أوجدت الاتفاقية الاوروبية تقسيما جديدا نسبيا ، فقد تضمنت اربع طوائف رئيسة لجرائم الكمبيوتر والانترنت .

الاولى : - الجرائم التي تستهدف عناصر (السرية والسلامة وموفورية) المعطيات والنظم وتضم :-

الدخول غير قانوني (غير المصرح به) .

الاعتراض غير القانوني .

تدمير المعطيات .

اعتراض النظم .

اساءة استخدام الاجهزة .

الثانية : الجرائم المرتبطة بالكمبيوتر وتضم : -

التزوير المرتبط بالكمبيوتر .

الاحتيال المرتبط بالكمبيوتر .

الثالثة : الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالافعال الاباحية واللاأخلاقية .

الرابعة : الجرائم المرتبطة بالاخلال بحق المؤلف والحقوق المجاورة – قرصنة البرمجيات .

تصنيف الجرائم تبعا لمساسها بالاشخاص والاموال .

نجد هذا التصنيف شائعا في الدراسات والابحاث الامريكية – مع فروق بينها من حيث مشتملات التقسيم ومدى انضباطيته ، كما نجده المعيار المعتمد لتقسيم جرائم الكمبيوتر والانترنت في مشروعات القوانين النموذجية التي وضعت من جهات بحثية بقصد محاولة ايجاد الانسجام بين قوانين الولايات المتحدة المتصلة بهذا الموضوع ويعكس هذا الاتجاه التقسيم الذي تضمنه مشروع القانون النموذجي لجرائم الكمبيوتر والانترنت الموضوع عام 1998 الذي تم وضعه من قبل فريق بحثي اكاديمي ، والمسمى **Model State Computer Crimes Code** ، وفي نطاقه تم تقسيم جرائم الكمبيوتر والانترنت الى ، الجرائم الواقعة على الاشخاص ، والجرائم الواقعة على الاموال عدا السرقة ، وجرائم السرقة والاحتيال ، وجرائم التزوير ، وجرائم المقامرة والجرائم ضد الاداب – عدا الجرائم الجنسية ، والجرائم ضد المصالح الحكومية ويلاحظ ان التقسيم يقوم على فكرة الغرض النهائي او المحل النهائي الذي يستهدفه الاعتداء ، لكنه ليس تقسيما منضبطا ولا هو تقسيم محدد الاطر ، فالجرائم التي تستهدف الاموال تضم من حيث مفهومها السرقة والاحتيال ، اما الجرائم التي تستهدف التزوير فتمس الثقة والاعتبار ، والجرائم الواقعة ضد الاداب قد تتصل بالشخص وقد تتصل بالنظام والاخلاق العامة ، وعلى العموم فانه وتبعا لهذا التقسيم – الوارد ضمن مشروع القانون النموذجي الامريكي - تصنف جرائم الكمبيوتر على النحو التالي :-

1-3-3 طائفة الجرائم التي تستهدف الاشخاص :-

وتضم طائفتين رئيستين هما :-

1- الجرائم غير الجنسية التي تستهدف الاشخاص Non-Sexual Crimes Against Persons وتشمل القتل بالكمبيوتر Computer Murder ، والتسبب بالوفاة جرائم الاهمال المرتبط بالكمبيوتر Negligent Computer Homicide ، والتحريض على الانتحار Soliciting or Encouraging Suicide ، والتحريض القصدي للقتل عبر الانترنت Intentional Internet Homicide Solicitation والتحرش والمضايقة عبر وسائل الاتصال المؤتمتة Harassment via Computerized Communication والتهديد عبر وسائل الاتصال المؤتمتة Intimidation via Computerized Communication والاحداث المتعمد للضر العاطفي او التسبب بضرر عاطفي عبر وسائل التقنية Malicious Infliction of Emotional Distress utilizing Computer Communication و Reckless Infliction of Emotional Distress utilizing Computer Communication والملاحقة عبر الوسائل التقنية Stalking وانشطة اخلاس النظر او الاطلاع على البيانات الشخصية Online Voyeurism and Online Voyeurism Disclosure وقنابل البريد الالكتروني E-mail Bombing وانشطة ضخ البريد الالكتروني غير المطلوب او غير المرغوب به Spamming utilizing Computerized Communication وبث المعلومات المضللة او الزائفة Transmission of False Statements والانتهاك الشخصي لحرمة كمبيوتر (الدخول غير المصرح به) Personal trespass by computer

2- طائفة الجرائم الجنسية Sexual Crimes :- وتشمل حض وتحريض القاصرين على انشطة جنسية غير مشروعة Soliciting a Minor with a Computer for Unlawful Sexual Purposes وافساد القاصرين باشطة جنسية عبر الوسائل الالكترونية Corrupting a Minor with the use of a Computer for Unlawful Sexual Purposes. واغواء او محاولة اغواء القاصرين لارتكاب انشطة جنسية غير مشروعة Luring or Attempted Luring of a Minor by Computer for Unlawful Sexual Purposes وتلقي او نشر المعلومات عن القاصرين عبر الكمبيوتر من اجل انشطة جنسية غير مشروعة Receiving or Disseminating Information about a Minor by Computer for Unlawful Sexual Purposes والتحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية Sexually Harassing a minor by use of a Computer for Unlawful Sexual Purposes ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الانترنت بوجه عام وللقاصرين تحديدا Posting Obscene Material On The Internet. و Posting Or Receiving Obscene Material On The Internet و Trafficking In Obscene Material On The Internet و Sending Obscene Material To Minors Over The Internet ونشر الفحش والمساس بالحياء (هتك العرض بالنظر) عبر الانترنت Indecent Exposure On The Internet وتصوير او اظهار القاصرين ضمن انشطة جنسية Depicting Minors Engaged In Sexually Explicit Conduct--Pandering Obscenity Involving A Minor واستخدام الانترنت لترويج الدعارة بصورة قسرية او للاغواء او لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم Using the Internet for Compelling Prostitution و Using the Internet for Pimping و Using the Internet for Soliciting و Using the Internet for Promoting Prostitution و الحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في انشطة جنسية Unauthorized Appropriation of Identity, Image, or Likeness for Unlawful Sexual Purposes وبامعان النظر في هذه الاوصاف نجد انها تجتمع جميعا تحت صورة واحدة هي استغلال الانترنت والكمبيوتر لترويج الدعارة او اثارة الفحش واستغلال الاطفال والقصر في انشطة جنسية غير مشروعة .

2-3-3 طائفة جرائم الاموال – عدا السرقة - او الملكية المتضمنة انشطة الاختراق والاتلاف Property Damage (Other than Theft) and Crimes Involving Intrusions

وتشمل انشطة اقتحام او الدخول او التوصل غير المصرح به مع نظام الكمبيوتر او الشبكة اما مجردا او لجهة ارتكاب فعل اخر ضد البيانات والبرامج والمخرجات Aggravated Computer Trespass و Computer Trespass و Disorderly Persons Offense وتخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب الكمبيوتر Computer Vandalism وايذاء الكمبيوتر Computer Mischief واغتصاب الملكية Extortion وخلق البرمجيات الخبيثة والضارة Creation of Harmful Programs و نقلها عبر النظم والشبكات Transmission of Harmful Programs و واستخدام اسم النطاق او العلامة التجارية او اسم الغير دون ترخيص Cybersquatting وادخال معطيات خاطئة او مزورة الى نظام كمبيوتر Introducing False Information Into a Computer or Computer System و لاتعديل غير المصرح به لاجهزة ومعدات الكمبيوتر Unlawful Modification of Computer Equipment or Supplies والاتلاف غير المصرح به لنظم الكميوتر (مهام نظم الكمبيوتر الادائية) Unlawful Modification of Computer Equipment or Supplies وانشطة انكار الخدمة او تعطيل او اعتراض عمل النظام او الخدمات Unlawful Denial, Interruption, or Degradation of Access to Computer وUnlawful Denial, Interruption, or Degradation of Access to Computer Services وانشطة الاعتداء على الخصوصية Computer Invasion of Privacy (وهذه تخرج عن مفهوم الجرائم التي تستهدف الاموال لكنها تتصل بجرائم الاختراق) وافشاء كلمة سر الغير Disclosure of Another's Password والحيازة غير المشروعة للمعلومات

Misuse of Computer واساءة استخدام المعلومات و **Unauthorized Possession of Computer Information** **Information** و نقل معلومات خاطئة **Transmission of False Data** .

3-3-3 جرائم الاحتيال والسرقة Fraud and Theft Crimes

وتشمل جرائم الاحتيال بالتلاعب بالمعطيات والنظم **Fraud by Computer Manipulation** واستخدام الكمبيوتر للحصول على او استخدام البطاقات المالية للغير دون ترخيص **Using a Computer to Fraudulently Obtain and Use Credit Card Information** او تدميرها **Damaging or Enhancing Another's Credit Rating** والاختلاس عبر الكمبيوتر او بواسطته **Computer Embezzlement** وسرقة معلومات الكمبيوتر **Computer Information Theft** وقرصنة البرامج **Software Piracy** وسرقة خدمات الكمبيوتر (وقت الكمبيوتر) **Theft of Computer Services** وسرقة ادوات التعريف والهوية عبر انتحال هذه الصفات او المعلومات داخل الكمبيوتر **Computer Impersonation** .

4-3-3 جرائم التزوير Forgery

وتشمل تزوير البريد الالكتروني **Electronic Mail Forgery (E-Mail Forgery)** وتزوير الوثائق والسجلات **Document/Record Forgery** و تزوير الهوية **Identity Forgery** .

5-3-3 جرائم المقامرة والجرائم الاخرى ضد الاخلاق والاداب Gambling and Other Offenses Against Morality

وتشمل تملك وادارة مشروع مقامرة على الانترنت **Owning and Operating an Internet Gambling business** وتسهيل ادارة مشاريع القمار على الانترنت **Facilitating the operation of an Internet gambling business** وتشجيع مشروع مقامرة عبر الانترنت **Patronizing an Internet Gambling Business** واستخدام الانترنت لترويج الكحول ومواد الادمان للقصر **Using the Internet to provide liquor to minors** و **Using the Internet to provide cigarettes to minors** و **Using the Internet to provide prescription drugs** .

6-3-3 جرائم الكمبيوتر ضد الحكومة Crimes Against the Government ،

وتشمل هذه الطائفة كافة جرائم تعطيل الاعمال الحكومية وتنفيذ القانون **Obstructing enforcement of law or other government function** والاخفاق في الابلاغ عن جرائم الكمبيوتر **Failure to report a cybercrime** والحصول على معلومات سرية **Obtaining confidential government information** والاخبار الخاطيء عن جرائم الكمبيوتر **False Reports of Cybercrimes** والعبث بالادلة القضائية او التاثير فيها **Tampering with evidenc** و **Tampering with a Computer Source Document** وتهديد السلامة العامة **Endangering Public Safety** وبث البيانات من مصادر مجهولة **Anonymity** كما تشمل الارهاب الالكتروني **Cyber-Terrorism** والانشطة الثارية الالكترونية او انشطة تطبيق القانون بالذات **Cyber-Vigilantism**.

تصنيف الجرائم كجرائم الكمبيوتر وجرائم الانترنت .

ومن الطبيعي ان يكون ثمة مفهوم لجرائم ترتكب على الكمبيوتر وبواسطته قبل ان يشيع استخدام شبكات المعلومات وتحديدا الانترنت ، ومن الطبيعي ان تخلق الانترنت انماطا جرمية مستجدة او تاثر بالالية التي ترتكب فيها جرائم الكمبيوتر ذاتها بعد ان تحقق تشبيك الكمبيوترات معا في نطاق شبكات محلية واقليمية وعالمية ، او على الاقل تطرح انماط فرعية من الصور القائمة تختص بالانترنت ذاتها ، ومن هنا جاء هذا التقسيم ، وسنجد انه وان كان مبررا من حيث المنطلق فانه غير صحيح في الوقت الحاضر بسبب سيادة مفهوم نظام الكمبيوتر المتكامل الذي لا تتوفر حدود وفواصل في نطاقه بين وسائل الحوسبة (الكمبيوتر) ووسائل الاتصال (الشبكات) .

وفي نطاق هذا المعيار يجري التمييز بين الافعال التي تستهدف المعلومات في نطاق نظام الكمبيوتر ذاته – خلال مراحل المعالجة والتخزين والاسترجاع – وبين الانشطة التي تستهدف الشبكات ذاتها او المعلومات المنقولة عبرها ، وطبعا الانشطة التي تستهدف مواقع الانترنت وخوادمها من نظم الكمبيوتر الكبيرة والعملاقة او تستهدف تطبيقات واستخدامات وحلول الانترنت وما نشا في بيئتها من اعمال الكترونية وخدمات الكترونية .

وفي اطار هذه الرؤيا ، نجد البعض يحصر انشطة جرائم الانترنت بتلك المتعلقة بالاعتداء على المواقع وتعطيلها او تشويهها او تعطيل تقديم الخدمة (انشطة انكار الخدمة السابق بيانها وانشطة تعديل وتحوير محتوى المواقع او المساس بعنصري الموفورية والتكاملية او سلامة المحتوى) وكذلك انشطة المحتوى الضار ، كترويج المواد الاباحية والمقامرة ، وانشطة اثارة الاحقاد والتحرش والازعاج ومختلف صور الانشطة التي تستخدم البريد الالكتروني والمراسلات الالكترونية ، وانشطة الاستيلاء على كلمات سر المستخدمين والهوية ووسائل التعريف ، وانشطة الاعتداء على الخصوصية عبر جمع المعلومات من خلال الانترنت ، وانشطة احتيال الانترنت كاحتيال المزادات وعدم التسليم الفعلي للمنتجات والخدمات ، وانشطة نشر الفايروسات والبرامج الخبيثة عبر الانترنت ، وانشطة الاعتداء على الملكية الفكرية التي تشمل الاستيلاء

على المواد والمصنفات المحمية واساءة استخدام اسماء النطاقات او الاستيلاء عليها او استخدامها خلافا لحماية العلامة التجارية وانشطة الاعتداء على محتوى المواقع والتصميم ، وانشطة الروابط غير المشروعة وانشطة الاطر غير المشروعة (وهي انشطة يقوم من خلالها احد المواقع باجراء مدخل لربط مواقع اخرى او وضعها ضمن نطاق الاطار الخارجي لموقعه هو ، وغيرها من الجرائم التي يجمعها مفهوم (جرائم الملكية الفكرية عبر الانترنت) .

اما جرائم الكمبيوتر فانها وفق هذا التقسيم تعاد الى الانشطة التي تستهدف المعلومات والبرامج المخزنة داخل نظم الكمبيوتر وتحديدا انشطة التزوير واحتيال الكمبيوتر وسرقة المعطيات وسرقة وقت الحاسوب واعتراض المعطيات خلال النقل (مع انه مفهوم يتصل بالشبكات اكثر من نظم الكمبيوتر) طبعا اضافة للتدخل غير المصرح به والذي يتوزع ضمن هذا التقسيم بين دخول غير مصرح به لنظام الكمبيوتر ودخول غير مصرح به للشبكات فيتبع لمفهوم جرائم الانترنت .

ولو وقفنا على هذا التقسيم فاننا بالضرورة ودون عناء سنجده تقسيما غير دقيق وغير منضبط على الاطلاق ، بل ومخالف للمفاهيم التقنية وللمرحلة التي وصل اليها تطور وسائل تقنية المعلومات وعمليات التكامل والدمج بين وسائل الحوسبة والاتصال ، ففي هذه المرحلة ، ثمة مفهوم عام لنظام الكمبيوتر يستوعب كافة مكوناته المادية والمعنوية المتصلة بعمليات الادخال والمعالجة والتخزين والتبادل ، مما يجعل الشبكات وارتباط الكمبيوتر بالانترنت جزء من فكرة تكاملية النظام ، هذا من جهة ، ومن جهة اخرى ، فان انشطة الانترنت تتطلب اجهزة كمبيوتر تقارف بواسطتها ، وهي تستهدف ايضا معلومات مخزنة او معالجة ضمن اجهزة كمبيوتر ايضا هي الخوادم التي تستضيف مواقع الانترنت او تديرها ، واذا اردنا ان نتحكم في فصل وسائل تقنية المعلومات ، فان هذا لن يتحقق لان الشبكات ذاتها عبارة عن حلول وبرمجيات وبروتوكولات مدمجة في نظام الحوسبة ذاته الا اذا اردنا ان نحصر فكرة الشبكات بالاسلاك واجهزة التوجيه (الموجهات) ، وهذا يخرجنا من نطاق جرائم الكمبيوتر والانترنت الى جرائم الاتصالات التي تستهدف ماديات الشبكة ، مشيرين هنا ان الموجهات التي قد يراها البعض تجهيزات تتصل بالشبكة ما هي في الحقيقة الا برامج تتحكم بحركة تبادل المعطيات عبر الشبكة .

ويعدو المعيار غير صحيح البتة اذا ما عمدنا الى تحليل كل نمط من انماط الجرائم المتقدمة في ضوؤ هذا المعيار ، فعلى سبيل المثال ، تعد جريمة الدخول غير المصرح به لنظام الكمبيوتر وفق هذا المعيار جريمة كمبيوتر اما الدخول غير المصرح به الى موقع انترنت فانها جريمة انترنت ، مع ان الحقيقة التقنية ان الدخول في الحالتين هو دخول الى نظام الكمبيوتر عبر الشبكة . ولو اخذنا مثلا جريمة انكار الخدمة وتعطيل عمل النظام ، فسواء وجهت الى نظام كمبيوتر ام موقع انترنت فهي تستهدف نظام الكمبيوتر الذي هو في الحالة الاولى كمبيوتر مغلق وفي الثانية كمبيوتر يدير موقع انترنت .

ولكل من الصور المتقدمة اركان وصور فرعية ووسائل فنية لا يتسع المقام لعضها وسنعمد على التركيز على ابرز هذه المسائل خلال محاضراتنا في المؤتمر ، مكتفين بايراد هذه التقسيمات ومحيلين القاريء الكريم بشان عناصر واركان كل جريمة الى مؤلفنا جرائم الكمبيوتر والانترنت الذي عالجها تفصيلا مع استعراض ابرز الحالات التطبيقية بشانها .؟

4- حالات عملية شهيرة من واقع الملفات القضائية .

والاحداث الشهيرة في هذا الحقل كثيرة ومتعددة لكننا نكتفي في هذا المقام بايراد ابرز الحوادث التي حصلت خلال السنوات الماضية بحيث نعرض لحوادث قديمة نسبيا وحديثة كامثلة على تنامي خطر هذه الجرائم وتحديدا في بيئة الإنترنت .

قضية مورس:- هذه الحادثة هي أحد اول الهجمات الكبيرة والخطرة في بيئة الشبكات ففي تشرين الثاني عام 1988 تمكن طالب يبلغ من العمل 23 عاما ويدعى ROBER MORRIS من اطلاق فايروس عرف باسم (دودة مورس) عبر الإنترنت ، أدى الى اصابة 6 آلاف جهاز يرتبط معها حوالي 60000 نظام عبر الإنترنت من ضمنها اجهزة العديد من المؤسسات والدوائر الحكومية ، وقد قدرت الخسائر لاعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار اضافة الى مبالغ اكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة ، وقد حكم على مورس بالسجن لمدة 3 اعوام وعشرة آلاف غرامة.

قضية الجحيم العالمي :- تعامل مكتب التحقيقات الفدرالية مع قضية اطلق عليها اسم مجموعة الجحيم العالمي GLOBAL HELL فقد تمكنت هذه المجموعة من اختراق مواقع البيت الابيض والشركة الفدرالية الأمريكية والجيش الامريكي ووزارة الداخلية الأمريكية ، وقد أدين اثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة ، وقد ظهر من التحقيقات ان هذه المجموعات تهدف الى مجرد الاختراق اكثر من التدمير او التقاط المعلومات الحساسة ، وقد امضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها ، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة .

فايروس ميلسا :- وفي حادثة هامة أخرى ، انخرطت جهات تطبيق القانون وتنفيذه في العديد من الدول في تحقيق واسع حول اطلاق فايروس شرير عبر الإنترنت عرف باسم فايروس MELISSA حيث تم التمكن من اعتقال مبرمج كمبيوتر من ولاية نيوجرسي في شهر نيسان عام 1999 واتهم باختراق اتصالات عامة والتآمر لسرقة خدمات الكمبيوتر ، وتصل العقوبات في الاتهامات الموجهة له الى السجن لمدة 40 عام والغرامة التي تقدر بحوالي 500 الف دولار وقد صدر في هذه القضية مذكرات اعتقال وتفتيش بلغ عددها 19 مذكرة .

حادثة المواقع الاستراتيجية :- وفي 19 تشرين الثاني 1999 تم ادانة **Eric burns** من قبل محكمة فيرجينيا الغربية بالحبس لمدة 15 شهرا والبقاء تحت المراقبة السلوكية لمدة 3 سنوات بعد ان اقر بذنبه وانه قام وبشكل متعمد باختراق كمبيوترات محمية الحق فيها ضررا بالغا في كل من ولايات فيرجينيا واشنطن واضافة الى لندن في بريطانيا ، وقد تضمن هجومه الاعتداء على مواقع لحلف الاطلسي اضافة الى الاعتداء على موقع نائب رئيس الولايات المتحدة كما اعترف بانه قد اطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق كمبيوترات البيت الابيض ، وقد قام **eric** بتصميم برنامج اطلق عليه **web bandit** ليقوم بعملية تحديد الكمبيوترات المرتبطة بشبكة الإنترنت التي تتوفر فيها نقاط ضعف تساعد على اختراقها ، وباستخدام هذا البرنامج اكتشف ان الخادم الموجود في فيرجينيا والذي يستضيف مواقع حكومية واستراتيجية منها موقع نائب الرئيس يتوفر فيه نقاط ضعف تمكن من الاختراق ، فقام في الفترة ما بين آب 1998 وحتى كانون الثاني 1999 باختراق هذا النظام 4 مرات ، واثر نشاطه على العديد من المواقع الحكومية التي تعتمد على نظام وموقع **USIA** للمعلومات ، وفي إحدى المرات تمكن من جعل آلاف الصفحات من المعلومات غير متوفرة مما أدى الى اغلاق هذا الموقع لثمانية ايام ، كما قام بالهجوم على مواقع لثمانين مؤسسة أعمال يستضيفها خادم شبكة **LASER.NET** في منطقة فيرجينيا والعديد من مؤسسات الاعمال في واشنطن اضافة الى جامعة واشنطن والمجلس الاعلى للتعليم في فيرجينيا رتشموند ومزود خدمات إنترنت في لندن ، وكان عادة يستبدل صفحات المواقع بصفحات خاصة به تحت اسم **ZYKLON** او باسم الامرأة التي يحبها تحت اسم **CRYSTAL** .

الاصدقاء الاعداء :- وفي حادثة أخرى تمكن أحد الهاكرز (الإسرائيليين) من اختراق أنظمة معلومات حساسة في كل من الولايات المتحدة الأمريكية والكيان الصهيوني ، فقد تمكن أحد المبرمجين الإسرائيليين في مطلع عام 1998 من اختراق عشرات النظم لمؤسسات عسكرية ومدنية وتجارية في الولايات المتحدة وإسرائيل ، وتم متابعة نشاطه من قبل عدد من المحققين في الولايات المتحدة الأمريكية حيث اظهرت التحقيقات ان مصدر الاختراقات هي كمبيوتر موجود في الكيان الصهيوني فانتقل المحققون الى الكيان الصهيوني وتعاونت معهم جهات تحقيق إسرائيلية حيث تم التوصل للفاعل وضبطت كافة الاجهزة المستخدمة في عملية الاختراق ، وبالرغم من ان المحققين أكدوا ان المخترق لم يتوصل الى معلومات حساسة الا ان وسائل الاعلام الأمريكية حملت أيضا أخبارا عن ان هذا الشخص كان في الاساس يقوم بهذه الانشطة بوصفه عميلا (لإسرائيل) ضد الولايات المتحدة الأمريكية.

حادثة شركة اوميغا :- مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لشركة **omega** من مدينة **Delaware** ويدعى **Timothy Allen Lioyd** (35 عاما) تم اعتقاله في 1998/2/17 بسبب إطلاقه قنبلة إلكترونية في عام 1996 **bomb** بعد 20 يوما من فصله من العمل استطاعت ان تلغي كافة التصاميم وبرامج الانتاج لاحد كبرى مصانع التقنية العالية في نيوجرسي والمرتبطة والمؤثرة على نظم تحكم مستخدمة في **nasa** والبحرية الأمريكية ، ملحقا خسائر بلغت 10 مليون دولار وتعتبر هذه الحادثة مثالا حيا على مخاطر جرائم التخريب في بيئة الكمبيوتر بل اعتبرت انها اكثر جرائم تخريب الكمبيوتر خطورة منذ هذه الظاهرة .

5- التحديات الاجرائية لجرائم الكمبيوتر والانترنت - تحديد عام

ان انشطة مكافحة جرائم الكمبيوتر والانترنت ابرزت تحديات ومشكلات جمة تغاير في جوانب كثيرة التحديات والمشكلات التي ترتبط بالجرائم التقليدية الاخرى :-

فهذه الجرائم لا تترك اثرا ماديا في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما ان مرتكبيها يملكون القدرة على اتلاف او تشويه او اضاعة الدليل في فترة قصيرة .

والتفتيش في هذا النمط من الجرائم يتم عادة على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات ، وقد يتجاوز النظام المشتبه به الى انظمة اخرى مرتبطة ، وهذا هو الوضع الغالب في ظل شيوع التشبيك بين الحواسيب وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والاقليمية والدولية على مستوى الدول ، وامتداد التفتيش الى نظم غير النظام محل الاشتباه يخلق تحديات كبيرة اولها مدى قانونية هذا الاجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لاصحاب النظم التي يمتد اليها التفتيش .

كما ان الضبط لا يتوقف على تحريز جهاز الكمبيوتر فقد يمتد من ناحية ضبط المكونات المادية الى مختلف اجزاء النظام التي تزداد يوما بعد يوم، والاهم ان الضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام او النظم المرتبطة بالنظام محل الاشتباه ، اي على اشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والاتلاف ، وهذه الحقائق تثير مشكلات متعددة ، منها المعايير المقبولة للضبط المعلوماتي ومعايير التحريز اضافة الى مدى مساس اجراءات ضبط محتويات نظام ما بخصوصية صاحبه – وان كان المشتبه به – عندما تتعدى انشطة الضبط الى كل محتويات النظام التي تضم عادة معلومات وبيانات قد يحرص على سريتها او ان تكون محل حماية بحكم القانون او لطبيعتها او تعلقها بجهات اخرى .

وادلة الادانة ذات نوعية مختلفة ، فهي معنوية الطبيعة كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ والبرمجيات ، وقد اثارت وتثير امام القضاء مشكلات جمة من حيث مدى قبولها وحجيتها والمعايير المتطلبة لتكون كذلك خاصة في ظل قواعد الاثبات التقليدية .

كما ان اختصاص القضاء بنظر جرائم الكمبيوتر والقانون المتعين تطبيقه على الفعل لا يحظى دائما بالوضوح او القبول امام حقيقة ان غالبية هذه الافعال ترتكب من قبل اشخاص من خارج الحدود او انها تمر عبر شبكات معلومات وانظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها ، وهو ما يبرز اهمية امتحان قواعد الاختصاص والقانون الواجب التطبيق وما اذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم ام يتعين افراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات في

حقل الاختصاص القضائي . ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد انشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود وما يحتاجه ذلك الى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية .

اذن فان البعد الاجرائي لجرائم الكمبيوتر والانترنت ينطوي على تحديات ومشكلات جمة ، عناوينها الرئيسة ، الحاجة الى سرعة الكشف خشية ضياع الدليل ، وخصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم ، وقانونية وحجية ادلة جرائم الكمبيوتر والانترنت ، ومشكلات الاختصاص القضائي والقانون الواجب التطبيق . والحاجة الى تعاون دولي شامل في حقل امتداد اجراءات التحقيق والملاحقة خارج الحدود ، وهذه المشكلات كانت ولا تزال محل اهتمام الصعيدين الوطني ام الدولي .

توجيهات عملية في ضبط وتفتيش انظمة الكمبيوتر والشبكات

ثمة في هذا المقام بعض التوجيهات ، لكنها ليست ذات قيمة دون التدخل التشريعي لافراد قواعد تفتيش وضبط خاصة على نحو ما قررته التشريعات الوطنية المقارنة والوثائق الدولية .

ان القاعدة الاولى ان التفتيش يتطلب مذكرة قضائية تجيز تفتيش أنظمة الكمبيوتر. واما اجراء التفتيش دون مذكرة قضائية او الحصول على بيانات من جهات ليست محلا للاشتباه لتعلقها بالمشتبه به ، فانها مسائل تثير الكثير من المعارضة خاصة في ظل ما تقرر من قواعد تحمي الخصوصية وتحمي حقوق الافراد وتوجب مشروعية الدليل وسلامة مصدره ، او تبطل كل اجراء يتم خلافا للقواعد الاصولية المتعلقة بالتفتيش والضبط المنصوص عليها في القانون ، وهي مسائل – طبعا تختلف احكامها باختلاف النظم القانونية - ينفذ من خلالها الجناة عند عدم اجازة القانون هذا المسلك الاستثنائي وعلى نحو يجعلنا متمسكين بضرورة عدم اللجوء الى هذا السلوك – حتى لو اتاح النظام القانوني المعني ذلك مع تحفظنا على مثل هذا الحكم لان المشروعية الاجرائية توجب تحقيق اقصى ضمانات للمتهم تتفق ومقتضيات قرينة البراءة – ونرى الاصرار على وجوب استصدار مذكرات التفتيش ، اما مشكلات التفتيش فان حلها وتجاوزها امر منوط بالقواعد القانونية المتعين سنها اضافة الى التزام جهات التفتيش الحيطة في توفير متطلبات القانون والحيطة في مراعاة بعض المسائل الفنية في هذا الشان – نورد بعضها تاليا - واخيرا أهمية مباشرته ممن تتوفر لديهم الخبرات الفنية الكفيلة بتحقيق التفتيش غرضه .

فاذا كان المحقق يعلم ابتداءا عن وجود الادلة المتصلة بجريمة ما ضمن احد انظمة الكمبيوتر او الشبكات ، وكان الجرم ابتداءا من طبيعة الجرائم الالكترونية ، فان مذكرة التفتيش يتعين ان تكون واضحة في تحديد النظام محل التفتيش وايراد اوسع وصف يغطي ما يعرفه المحقق سلفا وما يفترض انه يتصل بالمسائل التي يعرفها .

اما ان كان النظام او مكان وجود الدليل غير معروف في نطاق المكان محل التفتيش فيتعين ان تجيء عبارات مذكرة التفتيش عامة ما امكن حتى لا يكون نصها قيدا على نطاق التفتيش والضبط ، فعلى سبيل المثال يمكن ان تتضمن مذكرة التفتيش والضبط ((اجراء التفتيش والضبط لاي من او لكل سجل او معلومات توجد بصورة الكترونية او مادية او خطية موجودة في اي جهاز لتخزين المعطيات سواءا كان نظام كمبيوتر ايا كان وصفه او شبكة معلومات او وسائط تخزين او اجهزة اتصال او اية نظم معالجة وتخزين يمكن ان يوجد فيها الدليل)) لكن عمومية مذكرة التفتيش لا تعني عدم وجوب بيان السبب ومبرر التفتيش ، ولا تعني تجاوز الاجراء بذاته للقواعد القانونية المقررة لحماية الافراد ، خاصة اؤلئك الذين لا صلة مباشرة لهم بالمشتبه به او بفعله .

ومن حيث الاصل فان التحري والتفتيش في بيئة جرائم الكمبيوتر والانترنت يتوقف على مدى دقة مذكرة التفتيش ونطاقها المكاني ، ويتعين ان يحرص المحققون او جهات الضبط المكلفة بالتفتيش من قبل النيابة على ان تغطي مذكراتهم اي مكان توجد فيه هذه البينات الالكترونية في نطاق الاختصاص المكاني وبالنظر الى الشخص او الجهة التي يدور التفتيش بشأنها . وهنا تظهر اهم مشكلة في مسائل التفتيش بالنسبة الى اختراقات الانترنت او الاختراقات الخارجية ، اذ قد يتطلب التحري تفتيش انظمة كمبيوتر عائدة لجهات لا صلة لها بالفعل او نتيجته ، كتفتيش نظم مزودي خدمات الانترنت ، او تفتيش انظمة الخوادم خارج الحدود او الطلب من مالكيها ومديريها تزويد جهة التحقيق ببيانات معينة ، ولا يمكن ان يقبل قانونا ان تغطي مذكرات التفتيش مواطن ومواقع واماكن خارج صلاحية نظام العدالة المكانية ، ومن هنا نشات الحاجة الى تعاون دولي حقيقي في ميدان انشطة التحري والتحقيق والضبط والتفتيش خارج الحدود .

اما مسالة حاجة انشطة التفتيش للسرعة ومسالة قدرة الجناة على اخفاء الدليل فهي التي استوجبت التفكير بآلية استصدار اوامر الحفظ المستعجلة للجهات التي قد تتوفر لديها البيانات المرتبطة بنشاط المشتبه به (هذا بالنسبة للغير) ، ومعلوم انه لا يمكن الزام اية جهة بتقديم اية بيانات بشان الخدمات المقدمة للزبائن او علاقتهم به ، لان هذه البيانات في الاصل سرية ولا يجوز افشاؤها الا وفق القانون ، فان الحاجة تعدو ماسة للتدخل التشريعي لاتاحة مكنة وايضا آلية الضبط المستعجل للنظم المشتبه بها مع امر كف يد المشتبه به عن استخدام النظام فورا بمجرد البدء باجراءت التفتيش ، اضافة الى الحق في ضبط الاجهزة لاجراء التفتيش عليها في مقار التحقيق باستخدام التقنيات التي تتيح ذلك والتي قد لا تتوفر في مكان التفتيش ، خاصة اذا ما علمنا ان تفتيش جزء صغير جدا من الذاكرة قد يحتاج ساعات ، فكيف هو الحال وقد اصبحت ذاكرات الكمبيوترات قادرة على تخزين ملايين الملفات ، اضافة الى ان التفتيش الاولي قد لا يحل مشكلة الملفات المخباة او المحمية او المشفرة . لكن هذه الحلول في نطاق التفتيش تناقض القواعد المقررة قانونا في حقل ضمانات المتهم (اي المتهم المعلوماتي في حالتنا) وضمانات احترام حقوق الانسان والحريات الفردية وفي مقدمتها الخصوصية . فمثل هذه الاجراءت قد تؤدي الى كشف بيانات شخصية او كشف اسرار العمل او الوصول الى ملفات يحرص اصحابها على سريتها او تيح لهم القانون ذلك ، وتعدو المسالة اكثر خطورة عندما يمتد التفتيش الى نظم مرتبطة بالنظام موضوع الاشتباه ، فتطال ملفات وبيانات جهات لا علاقة لها بالجريمة قد تكون خاضعة لسرية مهنية او

قواعد حماية سرية بيانات العملاء كما في حالة نظم الكمبيوتر الخاصة بمزودي الخدمات او نظم كمبيوترات البنوك او الجهات الصحية او اعمال المحاماة او غيرها .

ان الحاجة الى التنظيم التشريعي لجوانب الضبط والتفتيش في حقل جرائم الكمبيوتر ومسائل حماية البيانات الشخصية ايضا ، تجد موجبها في الحاجة الى توفير معيار مقبول يقيم توازنا بين حقوق وحريات الافراد وحماية خصوصياتهم ، وبين موجبات المكافحة وحاجتها الى قواعد استثنائية فرضتها تحديات هذه الجرائم التي تزيد عن تحديات غيرها .

ففي ظل سرعة اتلاف الدليل وطبيعة ما يثبت الجريمة ذاتها من الادلة ، وفي ظل الحاجة للتدخل السريع لضبط متعلقات الجريمة ، وفي ظل ارتباط مادة الجريمة او وسيلتها بانظمة اطراف اخرى لا صلة لهم بها او بشبكات ونظم معلومات خارج الحدود ، فان المكافحة الفاعلة قد تنطوي على اهدار لحقوق وحريات الكثيرين والتفريط بضمانات المتهم وما توجبه قرينة البراءة المقررة له ، وهذا التناقض لا مجال لفضه الا باقامة معيار تعكسه القواعد التشريعية، فالاستثناء على الحرية والقيد المقرر عليها يعدو مقبولا في ضوء اعتبارات مصلحة المجتمع وامنه متى ما توفر بحق هذا المبرر ومتى ما كان المعيار مدركا ان الاستثناء لا يجوز التوسع فيه ويتعين تقييده بالقيد التشريعي الواضح الذي لا يتيح للسلطات التغول بما منحها القانون من حقوق او بما تفسره هي وفق رؤيتها لما قرره القانون لها من صلاحيات .